

(12) UK Patent Application (19) GB (11) 2 182 176 (13) A

(43) Application published 7 May 1987

(21) Application No 8523622

(22) Date of filing 25 Sep 1985

(71) Applicant
NCR Corporation,

(Incorporated in USA-Maryland),

Dayton, Ohio 45479, United States of America

(72) Inventors

Theodoor Adriaan Kleijne,
Jan Bart Goossens,
Johannes Antonius Jozef de Bruin

(74) Agent and/or Address for Service

D. Millichap, International Patent Department, NCR
Limited, 206 Marylebone Road, London NW1 6LY

(51) INT CL⁴
G06F 12/14

(52) Domestic classification (Edition I)
G4AAP

(56) Documents cited
EP A 0142013 DE A 3023427
WO A 84/04614 US 4262329

(58) Field of search
G4A
Selected US specifications from IPC sub-class G06F

(54) Data security device for protection stored data

(57) The security device, for protecting sensitive data stored in a resettable memory, includes a housing formed of six ceramic plates (P1-P6) each having provided thereon a pair of thin film conductive path segments arranged in a meandering configuration. The thin film conductive path segments are joined together by interconnection devices each including a pair of ceramic studs (e.g. K9, K10) having conductive areas thereon connected by an interconnect block (e.g. N5), thereby forming two complete thin film conductive paths which meander in a closely spaced, parallel manner over the entire inner surface of the housing. Interrupting or short circuiting the thin film conductive paths causes reset means to reset the resettable memory thereby erasing the data stored therein.

The plates together define a ceramic housing which is resistant to chemical attack, physical attack and tempering at extremely low temperatures. Cutting or drilling the housing causes it to break or crack with consequential damage interrupting one or more conductive paths.

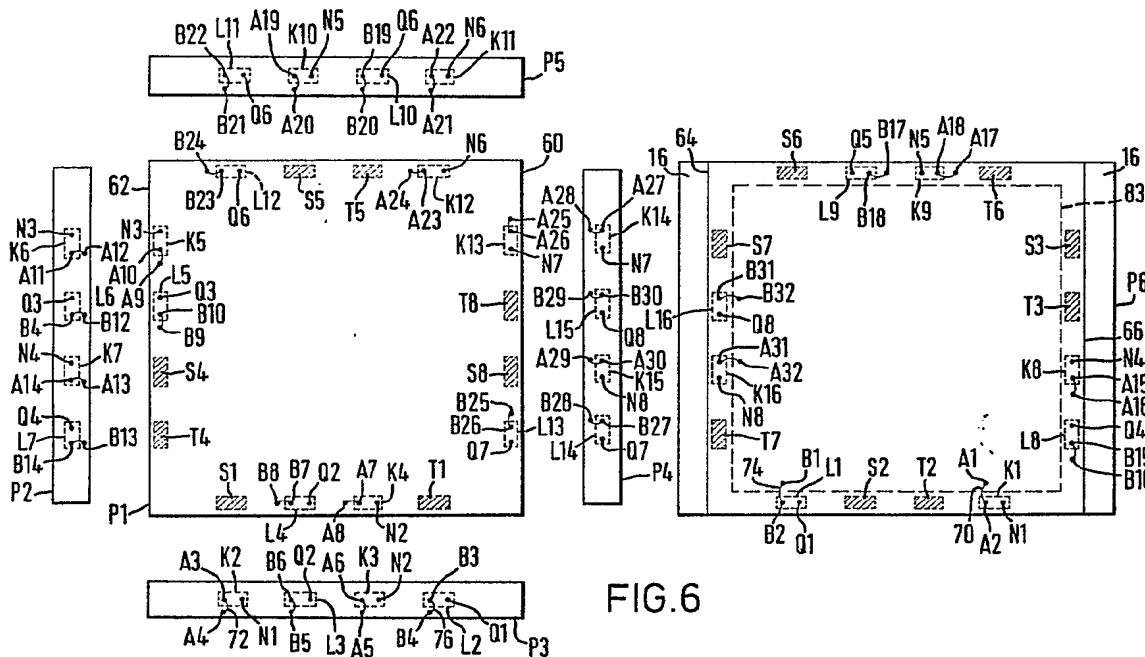


FIG.6

GB 2 182 176 A

1 / 8

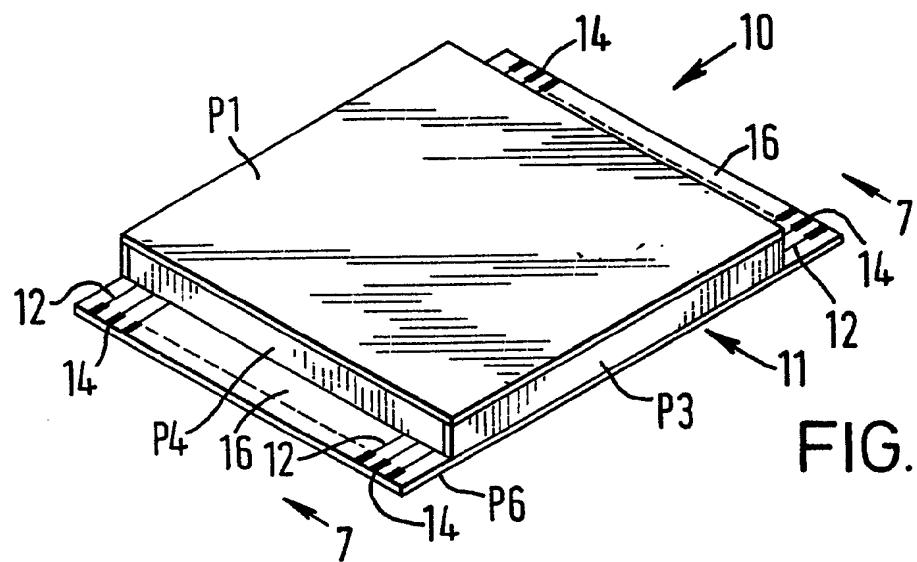


FIG. 1

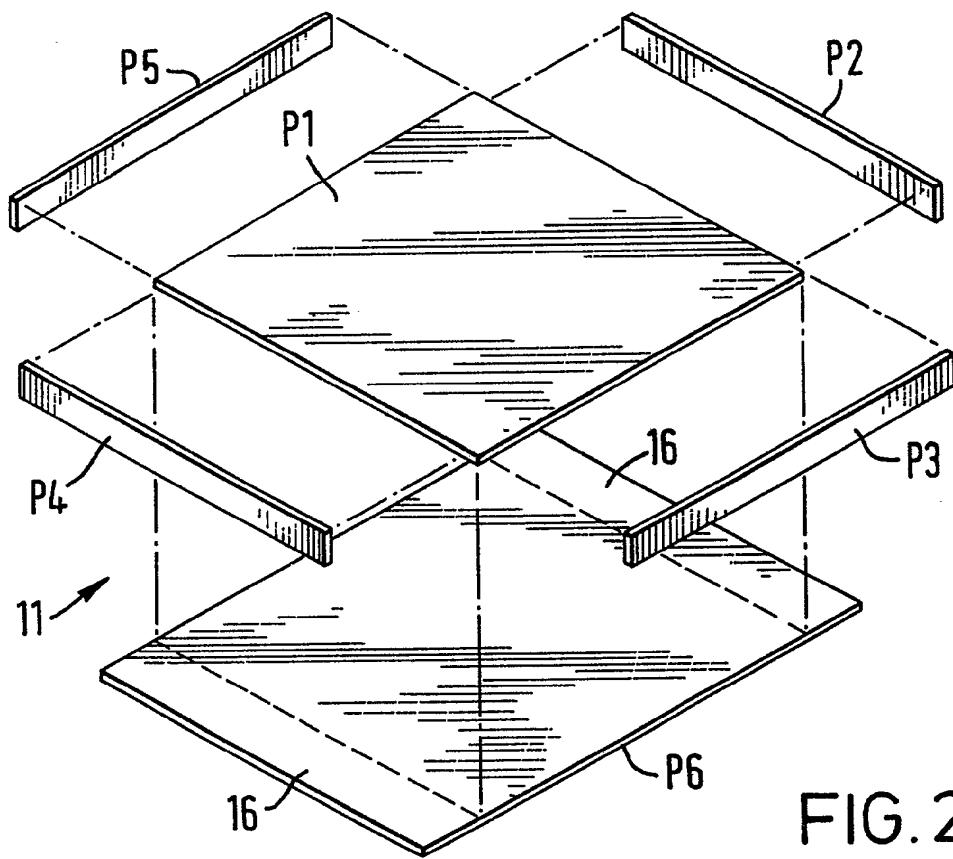
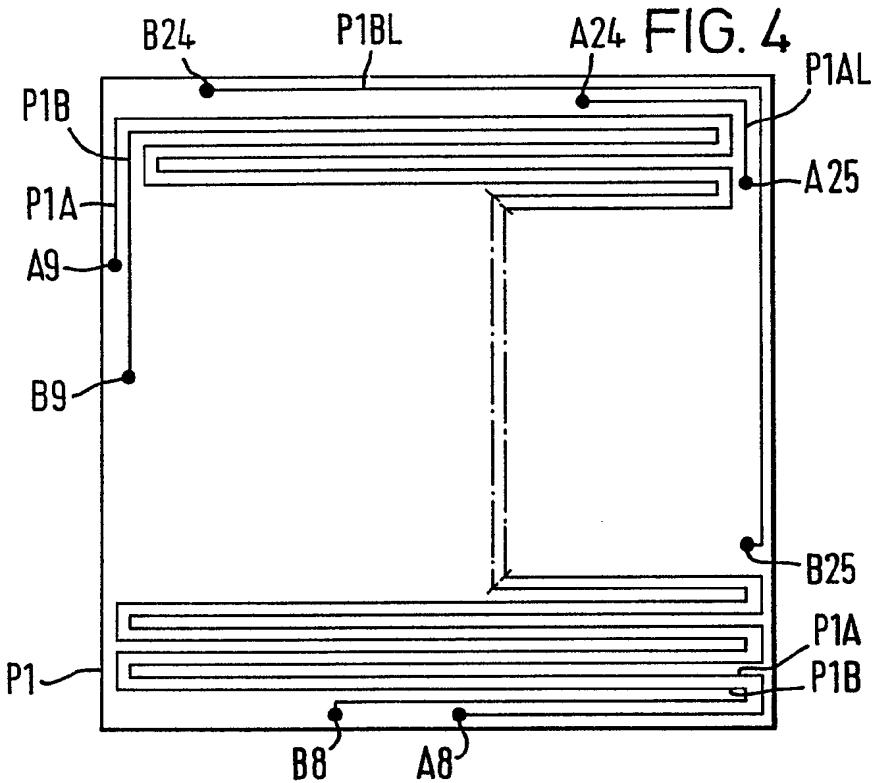
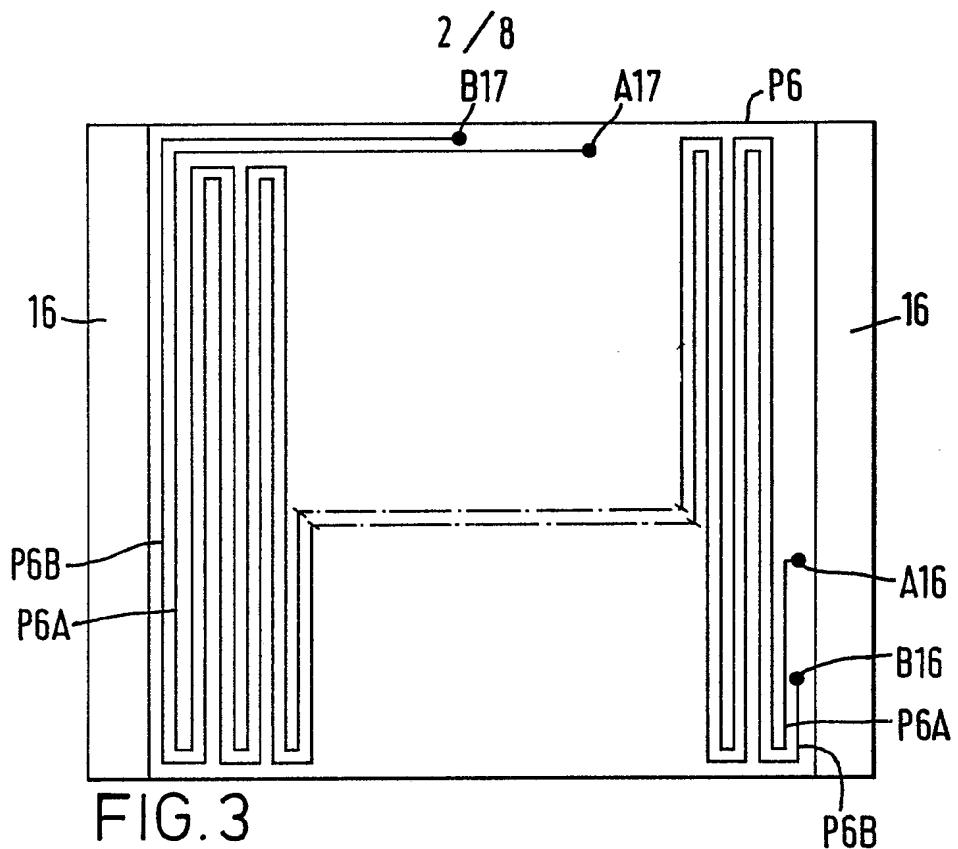


FIG. 2

2182176



2182176

3 / 8

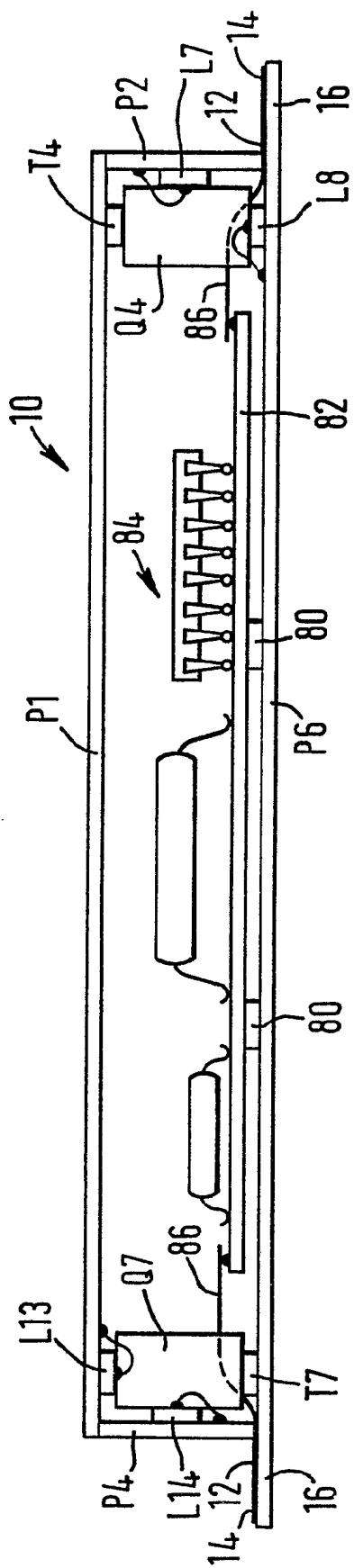


FIG. 7

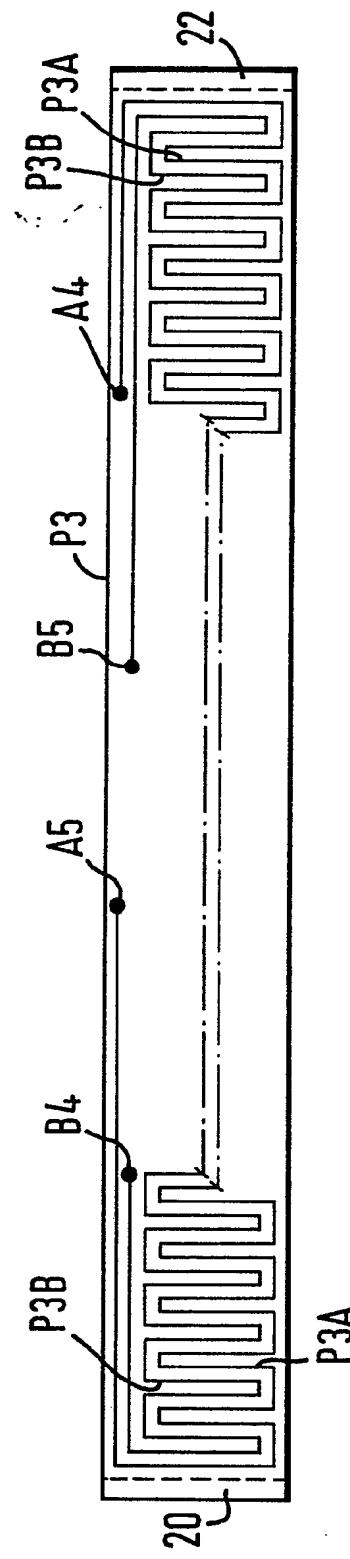


FIG.

2182176

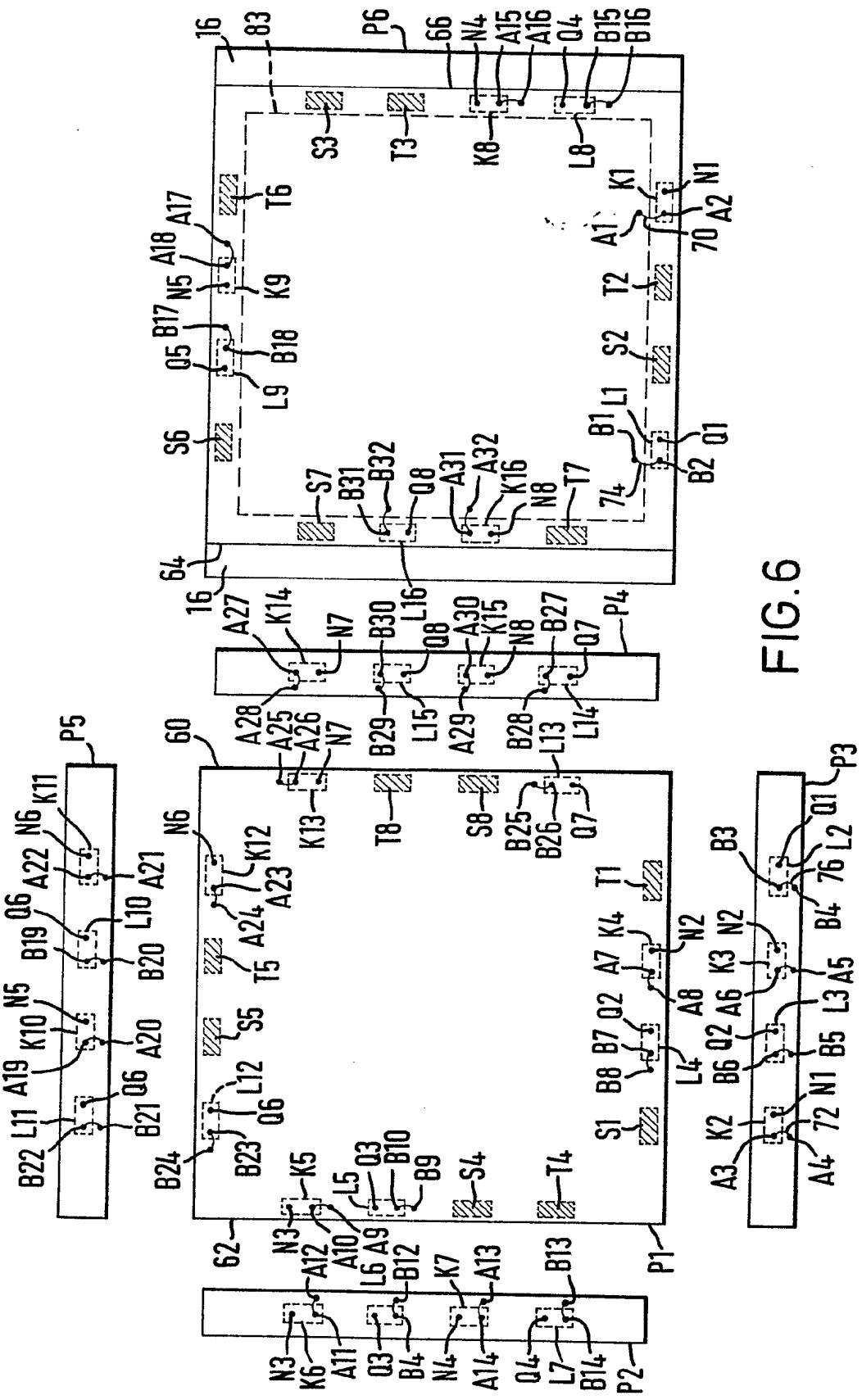


FIG. 6

5 / 8

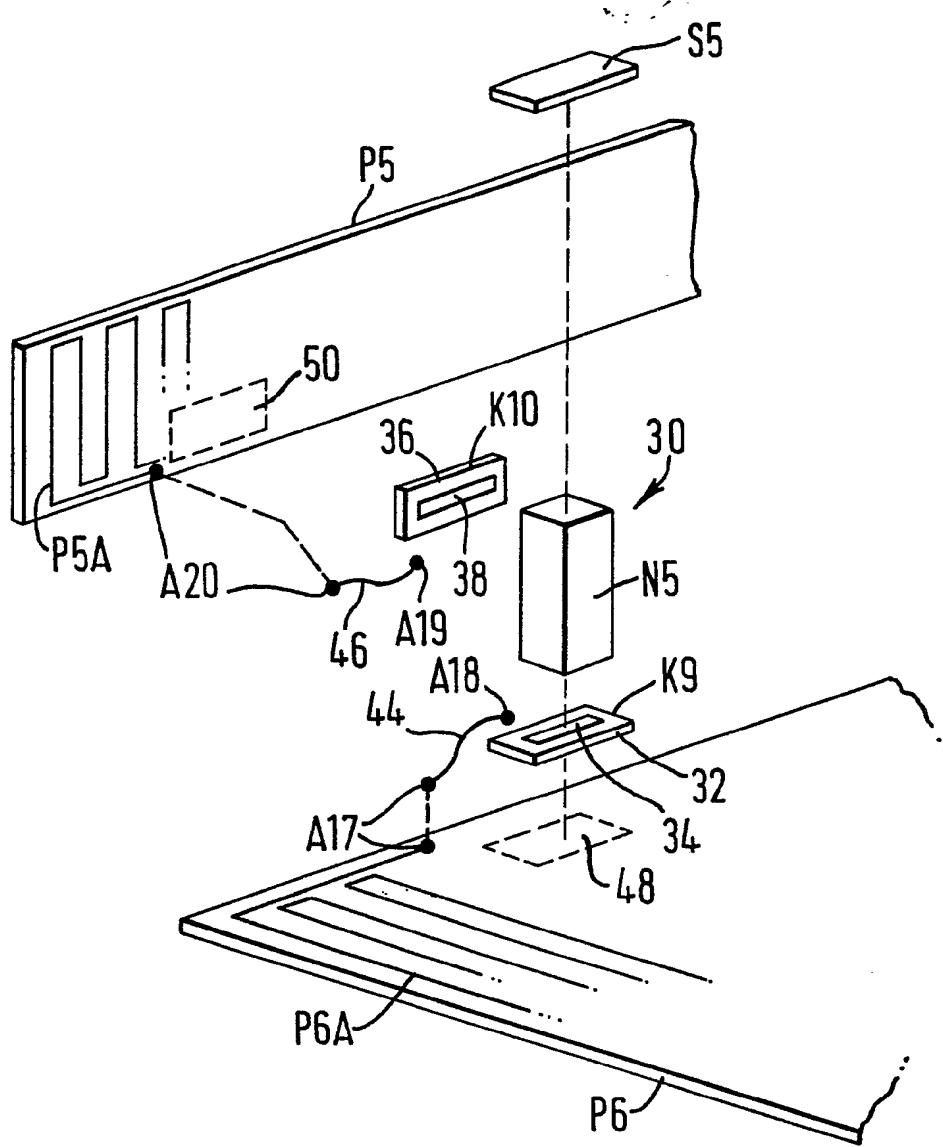


FIG. 8

6 / 8

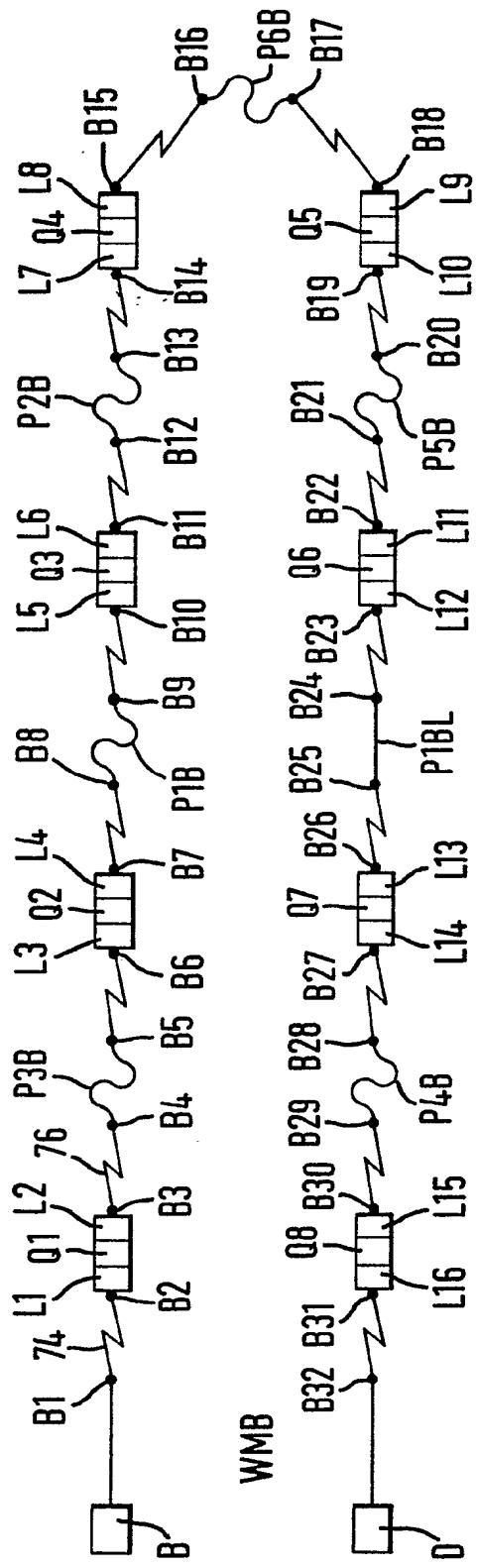
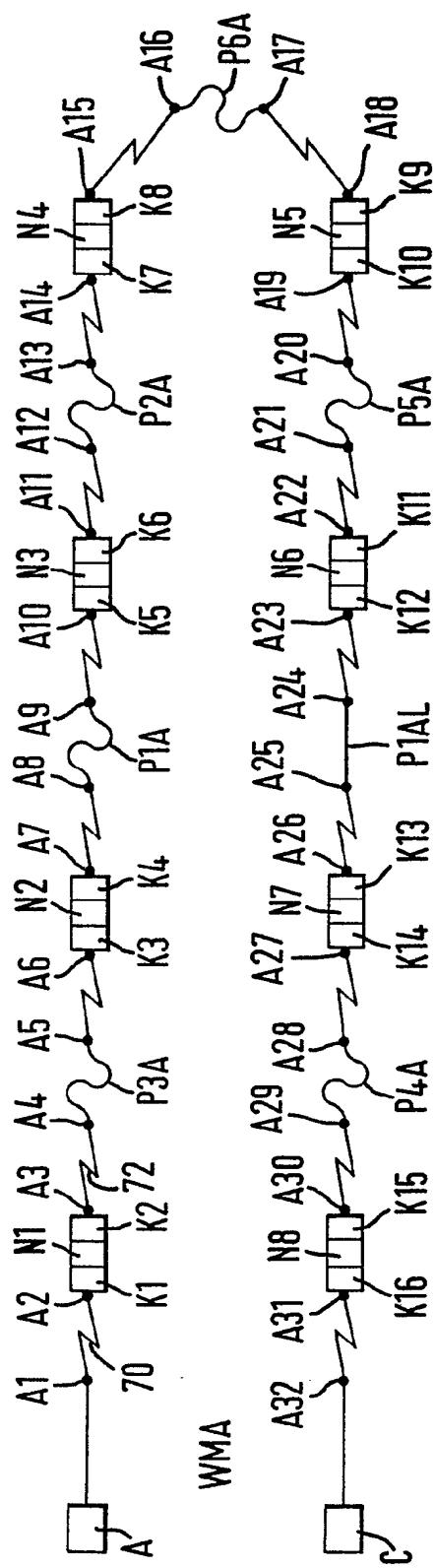


FIG. 9

FIG. 10

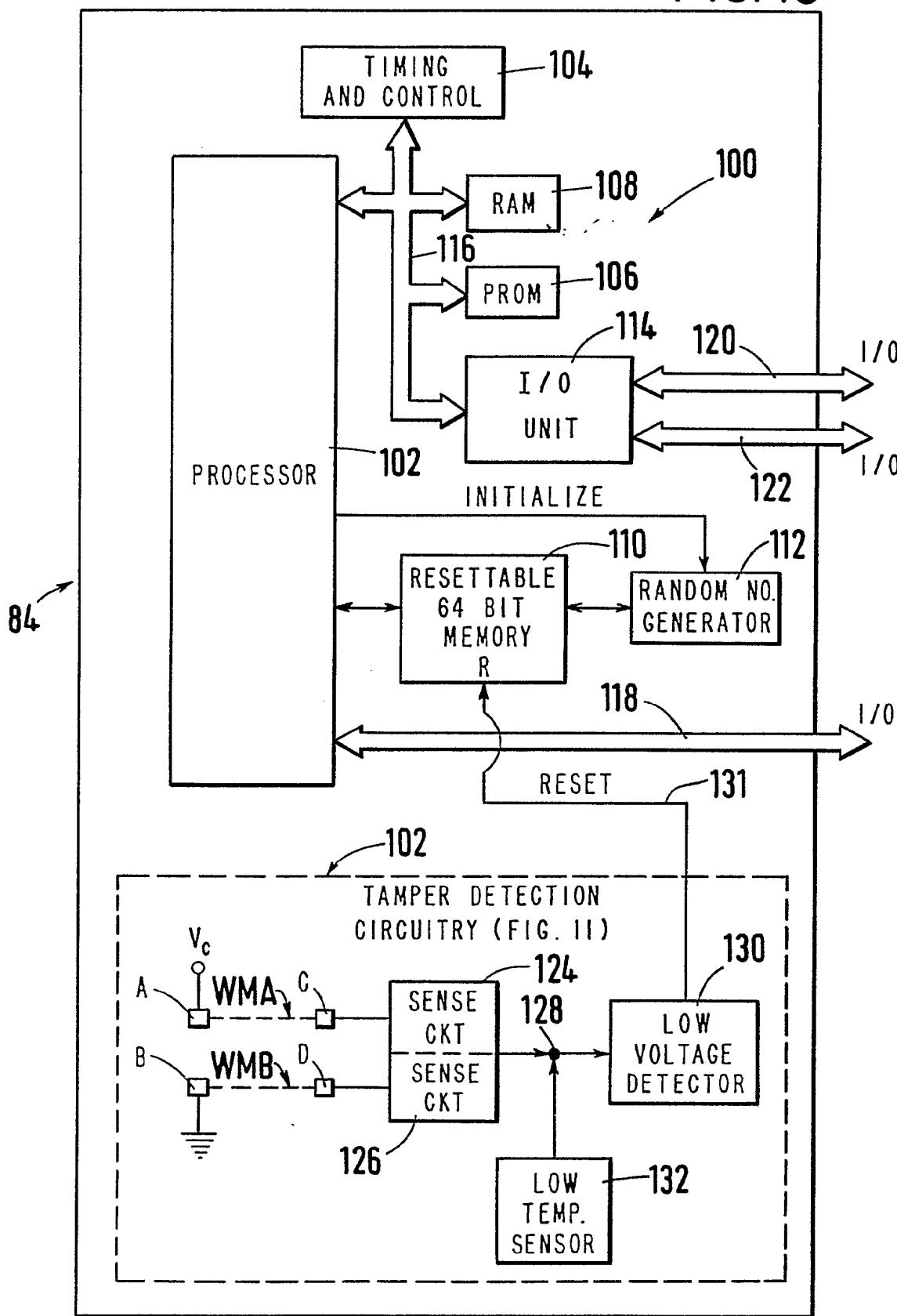
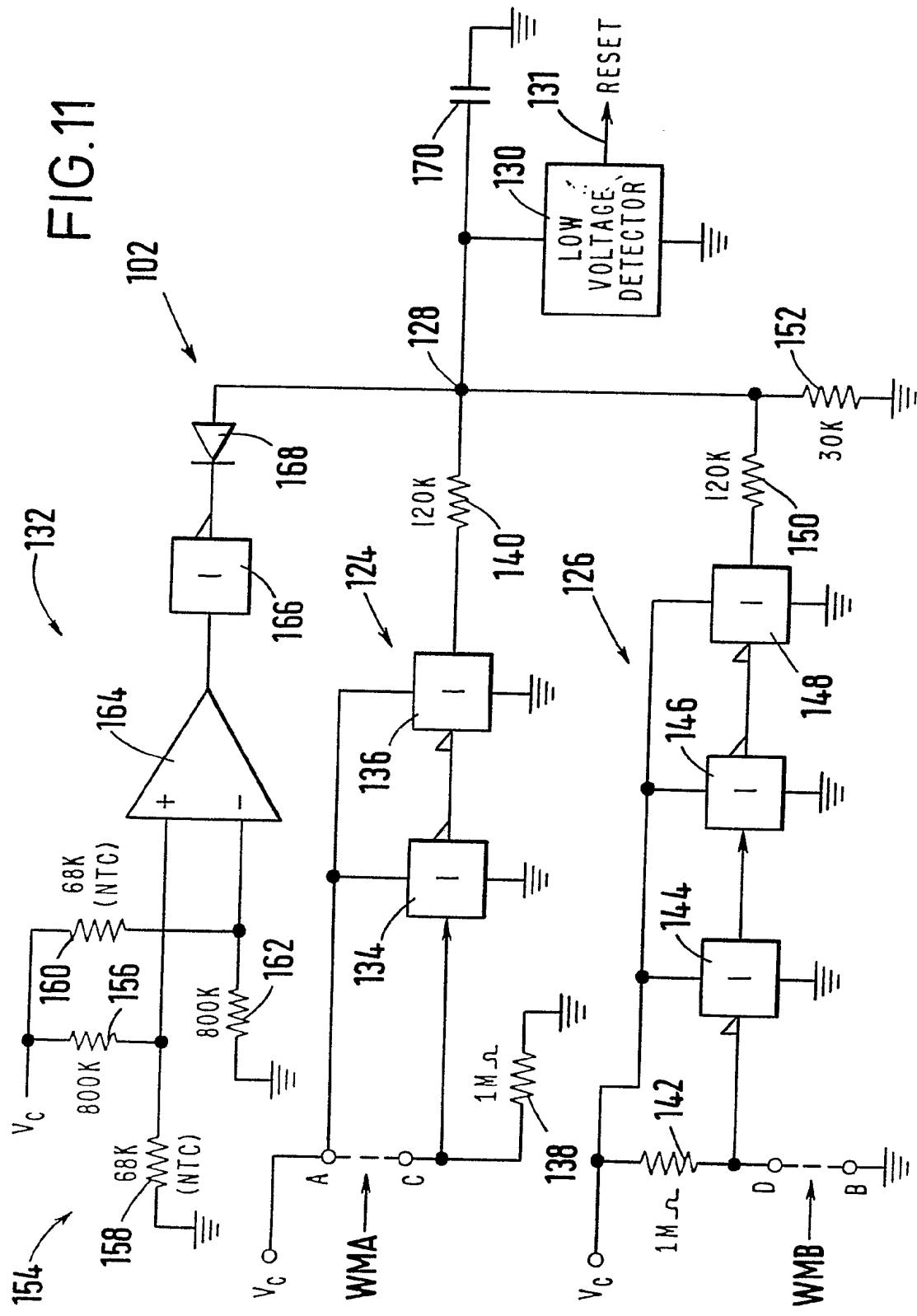


FIG. 11



SPECIFICATION

Data security device for protecting stored data

5 This invention relates to a security device for protecting stored sensitive data.

International Patent Application No. WO 84/04614 discloses a data security device which includes a container formed of a brittle material such as 10 pressed glass and which includes a data processor, a volatile CMOS RAM memory device for storing encryption key data, and a battery forming the power supply for the memory device. The container consists of a housing and a lid. The battery is connected 15 to the memory device by a power supply conductor formed in a winding path configuration on the interior surfaces of the housing and the lid, the parts of the power supply conductor on the housing and lid being connected by pairs of contacts at the joint faces 20 between the housing and the lid. The conductor is formed by an evaporated metal thin film material. The power supply conductor pattern is bifilar and the parts of the conductor are interleaved with additional conductors on the interior surfaces of the housing and lid which are earthed or connected to a voltage source. Thus, if the power supply conductor is 25 interrupted or connected to either of the additional conductors the power supply to the volatile RAM would be so much altered that the data in the RAM would be destroyed. The known device has the disadvantage of a relatively low level of security since the width of the power supply conductor provided on the housing must be maintained sufficiently great to enable the provision of an adequate power supply to 30 the memory device. Such relatively wide conductors are subject to the possibility of penetration. For example, it could be possible to produce a hole of sufficiently small diameter to maintain a conductive path in a relatively wide power supply conductor, yet 35 enable unauthorized access to the memory device via the hole.

German Offenlegungsschrift No. 3 023 427 discloses a mobile data storage unit which includes a plurality of memory devices within a closed container formed by a housing and a lid. Located within the material forming the walls of the container are a plurality of differential pressure sensing devices connected to closed channels also located in the walls of the container, such that any attempt to break into the 45 container which disrupts the pressure in the closed channels is detected by the pressure sensing devices and causes the operation of a relay to provide an erase signal to erase the contents of the memory devices. Also located within the material forming the 50 walls of the container are a pair of thin conductors, which run in an arbitrary configuration through the housing and the lid, and are connected to a power source and the relay. Any external influence which breaks either of these thin conductors also causes 55 the relay to provide an erase signal to erase the contents of the memory devices. However, this known device is of complex and expensive construction resulting from the provision of the closed channels and pressure sensing devices. Furthermore, the possibility exists of forming a small diameter hole into 60 65

the interior of the unit without interrupting either of the pair of thin conductors. Thus, the degree of security achievable with this known unit is also limited.

It is an object of the present invention to provide a 70 data security device wherein the aforementioned disadvantage is alleviated.

Therefore, according to the present invention, there is provided a security device for protecting stored sensitive data, including a closed housing containing 75 memory means adapted to store sensitive data, and conductive path means provided in a winding configuration on the entire inner surface of said housing, wherein said housing contains tamper detection circuitry which is coupled to said conductive path means and to said memory means, and which includes reset signal generating means adapted to generate a reset signal to erase the contents of said memory means in the event of an interruption of said conductive path means brought about by an attempt 80 to penetrate said housing.

Preferably, the conductive path means includes first and second substantially parallel conductive paths provided on the inner surface of the housing. It will be appreciated that this feature provides an 90 additional advantage over the data security device disclosed in the aforementioned International Patent Application No. WO 84/04614, wherein the formation of a small diameter hole through one of the earthed or powered additional conductors interleaved with 95 the power supply conductor would, of course, not affect the power supply to the volatile RAM, even if the hole completely interrupts the electrical continuity of the additional conductor. With the arrangement of the preferred feature, the interruption of 100 either of the first and second conductive paths produces a reset signal to erase the contents of the memory means.

It will be appreciated that the present specification refers to the techniques of thin film technology and 105 thick film technology. As is well known to those skilled in the electronics art, the former is a technology wherein a thin film, up to a few micrometres in thickness, is deposited by thin film deposition techniques. One such technique is to drop molten conductive metal on to a rapidly spinning substrate. Other techniques for forming thin films are vacuum evaporation and cathode sputtering. Such a deposited thin film is then etched to a desired configuration or pattern. Thin film technology is to be contrasted 110 with thick film technology wherein a paste is deposited by thick film deposition techniques, such as screen printing, and then fired, that is, heated to a sufficiently high temperature to harden the deposited paste, thereby forming a relatively thick film having 115 a thickness of the order of ten micrometres to a few tens of micrometres. Both thin film technology and thick film technology are well known to those skilled in the electronics art, and detailed description thereof is not considered necessary.

120 One embodiment of the present invention will now be described by way of example with reference to the accompanying drawings, in which:-

Figure 1 is a view of a security device according to the invention;

130 *Figure 2* is an exploded perspective view of the sec-

urity device shown in Figure 1;

Figure 3 is a schematic view showing on an enlarged scale two conductive path segments formed on the interior surface of the base plate of the security device shown in Figure 1;

Figure 4 is a schematic view showing on an enlarged scale two conductive path segments formed on the interior surface of the top plate of the security device shown in Figure 1;

10 *Figure 5* is a schematic view showing on an enlarged scale two conductive path segments formed on the interior surface of one of the side plates of the security device shown in Figure 1;

Figure 6 is a schematic view showing the manner in which the interconnections between the conductive path segments on the respective interior surfaces of the six plates forming the housing of the security device shown in Figure 1 are formed;

Figure 7 is an end view on an enlarged scale of the interior of the security device shown in Figure 1 looking along the direction of the arrows 7-7 in Figure 1, with the front side plate removed;

Figure 8 is an exploded perspective view showing the construction of one of the interconnection devices;

Figure 9 shows the manner in which the conductive path segments on the interior surfaces of the six plates are interconnected to form two complete conductive paths;

30 *Figure 10* is a block diagram of the electronic circuitry within the security device shown in Figure 1; and

Figure 11 is a circuit block diagram of the tamper detection circuitry of Figure 9.

Referring first to Figures 1 and 2 of the drawings, a security device 10 according to the invention includes a housing 11 which is formed by a top plate P1, side plates P2-P5 and a base plate P6. The six plates P1-P6 are preferably formed of a ceramic material since ceramic material is highly resistant to chemical attack. Included within the security device 10 is electronic circuitry (not shown in Figures 1 and 2), connected via conductive paths 12 to terminal areas 14 provided on end portions 16 of the base plate P6. The terminal areas 14 are in contact with respective conductive input-output pins (not shown) in a conventional manner to enable connections to external circuitry to be made by mounting the security device 10 on a printed circuit board.

Referring to Figures 3-7, the construction of the device 10 will now be described. Each of top plate P1, the side plates P2-P5 and the bottom plate P6 forming the housing 11, is provided on its interior surface with a pair of conductive path segments formed in a winding configuration with the paths on the various plates P1-P6 being connected together in a manner to be described hereinafter to form two complete conductive paths referred to herein as wire mesh A (WMA) and wire mesh B (WMB). Thus, referring to Figure 3, the bottom plate P6 is provided with conductive path segments P6A and P6B; referring to Figure 4, the top plate P1 is provided with conductive path segments P1A and P1B; and referring to Figure 5, the side plate P3 is provided with conductive path segments P3A and P3B. The conductive path segments P6A, P1A and P3A form part of WMA, and the

conductive path segments P6B, P1B and P3B form part of WMB. The conductive path segments on the side plates P2, P4 and P5 have an identical configuration to that shown for side plate P3 in Figure 5, the

70 side plates P2, P4 and P5 being provided with conductive path segments P2A, P2B; P4A, P4B; and P5A, P5B. The conductive path segments on all the side plates have identical configurations. It should be noted, however, that the side plates P2 and P4 have a slightly shorter length than the side plates P3 and P5, the end portions 20, 22 being absent. Thus, when the housing 11 of the device 10 is assembled the side plates P2 and P4 are attached to the end portions 20 and 22 of the side plates P3 and P5.

80 It will be appreciated that the precise configuration of the conductive path segments such as P1A, P1B, . . . , P6A, P6B is not of importance, and for reasons of clarity, has been shown only schematically in Figures 3, 4 and 5. Suffice it to say that the path segments of

85 the wire meshes WMA and WMB are disposed in an adjacent, coplanar, parallel relationship and form a winding configuration over substantially the entire surfaces of the respective plates P1-P6, with the exception of the end portions 16 of the base plate P6

90 and the end portions 20, 22 of the side plates P3 and P5. The winding configurations may be meandering paths which meander back and forth over the plate surfaces, as indicated in Figures 3, 4 and 5. The conductive path segments have a width of about 25 micrometres and the spacing between adjacent conductive segments is also about 25 micrometres. Furthermore, the thickness of the conductors of the conductive path segments is preferably within the range of about 0.5 micrometres to about 3.0 micrometres and

100 in the preferred embodiment is about 1.0 micrometres. If desired, the conductive path segments P1A, P1B, . . . , P6A, P6B could be coated with an insulating layer.

The manner in which the conductive path segments on the respective plates are interconnected will now be described with reference to Figure 8, which shows an exploded perspective view of a typical interconnection device 30 interconnecting the conductive path segments P5A and P6A on the plates

110 P5 and P6 respectively. The interconnection device 30 includes interconnect studs K9 and K10, an interconnect block N5 and a support stud S5. The interconnect stud K9 includes a nonconductive ceramic body 32 provided with a conductive area 34. The in-

115 terconnect stud K10 is of identical construction to the interconnect stud K9, and includes a nonconductive ceramic body 36 provided with a conductive area 38. The interconnect block N5 serves to provide an electrical interconnection between the conductive areas

120 34 and 38 on the interconnect studs K9 and K10 respectively. The interconnect block N5 may be formed of metal, but in the preferred embodiment includes a six sided block of non-conductive ceramic material, with two adjacent sides, that is, the sides facing the

125 interconnect studs K9 and K10 having conductive coatings provided thereon, such that a conductive path is established between the conductive areas 34 and 38. This has the advantage that the thermal coefficient of expansion of the interconnect block N5 is compatible with the other ceramic components of

the security device 10. The support stud S5 is of ceramic material and is located between the interconnect block N5 and the top plate P1 (not shown in Figure 8) when the housing 11 of the security device 5 10 is assembled.

An interconnection point A17 is formed by bonding one end of a wire 44 to the conductive path segment P6A on the plate P6. The other end of the wire 44 forms an interconnection point A18 by bonding to 10 the conductive area 34. An interconnection point A20 is formed by bonding one end of a wire 46 to the conductive path segment P5A on the plate P5. The other end of the wire 46 forms an interconnection point A19 by bonding to the conductive area 38. 15 The interconnection device 30 is assembled by bonding the interconnect studs K9, K10 to the respective plates P6, P5 by nonconductive epoxy, and bonding the interconnect block N5 to the conductive areas 34, 38 by conductive epoxy. The interconnect 20 block N5 is also bonded to the support stud S5 by nonconductive epoxy. The interconnect studs K9 and K10 are bonded by nonconductive epoxy to areas 48 and 50 on the respective plates P6 and P5. Bonding materials other than epoxy could be used. It should 25 be understood that the areas 48 and 50 overlie regions of the meandering coplanar conductive path segments P6A, P5A, P6B, P5B, although the conductive path segments P6B, P5B are not shown in Figure 8 for reasons of clarity. It will be appreciated that with 30 this arrangement the interconnection device 30 provides a very high degree of security against unauthorized attempts to break into the housing 11 of the security device 10 in the neighbourhood of an interconnection device such as the device 30.

35 Referring particularly to Figure 6, the interior surfaces of the six plates P1-P6 of the housing 11 are shown schematically. When assembled, the edges 60, 62 of the top plate will overlie the inner boundaries 64, 66, respectively, of the end portions 16 of the base plate P6. For clarity, the conductive path segments P1A-P6A and P1B-P6B are not shown in Figure 6.

The configuration of the wire meshes WMA and 45 WMB as embodied on the six plates P1-P6 so as to form winding path configurations over the entire inner surface of the housing 11, will be clarified by referring to Figure 6 in conjunction with Figure 9, which shows the wire mesh WMA formed between terminals A and C and the wire mesh WMB formed 50 between terminals B and D.

In more detail, the wire mesh WMA connects to interconnection point A1 (Figures 6 and 9), and thence via a conductive wire 70 to interconnection point A2 on the interconnect stud K1. The conductive wire 70 55 is bonded and connected in a similar manner to that described hereinabove for the wire 44 in Figure 8. For the sake of clarity, the conductive areas on the interconnect studs such as K1, to which the interconnections are made, are not specifically shown in Figure 6. The path proceeds from the interconnect stud K1 via the interconnect block N1 (schematically shown in Figure 6 as a pair of dark spots on the interconnect studs K1 and K2 respectively), the interconnect stud K2, the interconnection point A3, a conductive bonded wire 72 and an interconnection point

A4 which is connected to the conductive path segment P3A (not shown in Figure 6) on the plate P3. The support stud S1 is shown schematically as a shaded area on the plate P1. In Figure 9, the zigzag line configurations such as the zigzag line between inter-

connection points A5 and A6, represent conductive bonded wires similar to the conductive bonded wires 70 and 72. By following through the sequence shown for WMA in Figure 9, it will be seen that the wire mesh 70 WMA includes winding conductive path segments P3A, P1A, P2A, P6A and P5A on the plates P3, P1, P2, P6 and P5 in sequence, a conductive interconnect path P1AL between the interconnection points A24 and A25 (see Figure 4) on the plate P1 and a winding 75 conductive path segment P4A on the plate P4. The physical location of the interconnect studs K1-K16 and the interconnect blocks N1-N8 is clear from Figure 6, which also shows the locations of the support studs S1-S8 for the interconnect blocks N1-N8. 80 The interconnect studs K1-K16 are all of identical construction to the interconnect studs K9 and K10 described hereinabove with reference to Figure 8.

The configuration of the wire mesh WMB is identical to that just described for the wire mesh WMA.

90 Thus, the path from terminal B connects to interconnection point B1 (Figures 6 and 9), and thence via a conductive wire 74 bonded to interconnection point B2 on an interconnect stud L1. The path proceeds from the interconnect stud L1 via an inter- 95 connect block Q1 (schematically shown as a pair of dark spots on the interconnect studs L1 and L2 respectively), the interconnect stud L2, the interconnection point B3, a conductive wire 76 and an interconnection point B4 which is connected to the

100 conductive path segment P3B (not shown in Figure 6). The support stud T1 is shown schematically as a shaded area on the plate P1. By following through the sequence shown for WMB in Figure 9, it will be seen that the wire mesh WMB includes winding conduct-

105 ives path segments P3B, P1B, P2B, P6B and P5B on the plates P3, P1, P2, P6 and P5 in sequence, a conductive interconnect path P1BL between the interconnection points B24 and B25 on the plate P1 (see Figure 4) and a winding conductive path segment P4B on the plate 110 P4. The physical location of the interconnect studs L1-L16 and the interconnect blocks Q1-Q8 is clear from Figure 6, which also shows the location of the support studs T1-T8 for the interconnect blocks Q1-Q8.

115 Referring now particularly to Figure 7, an end view of the interior of the assembled security device 10 is shown. Mounted on the base plate P6 are ceramic studs 80 which support a ceramic plate 82 on which is mounted electronic circuitry shown generally by re-

120 ference 84. The location of the ceramic plate 82 is shown by the dashed rectangle 83 in Figure 6. The electronic circuitry 84, Figure 7, is connected via conventional flexible printed circuit connections 86 to the conductive paths 12 and hence to the terminal

125 areas 14. Also shown in Figure 7 are interconnect blocks Q4 and Q7, interconnect studs L7, L8, L13 and L14 mounted on the plates P2, P6, P1 and P4 respectively, and support studs T4 and T7 mounted on the plates P1 and P6 respectively. It will be appreciated that the terminals A, C, B, D (Figure 9) are inclu-

ded in the electronic circuitry 84, although not specifically shown in Figure 7.

The manner in which the security device 10 is manufactured will now be briefly described. The plates 5 P1-P6 are prepared in the following manner, utilizing known techniques of thin film technology. Firstly, a conductive thin film is deposited on a major surface of each of the ceramic plates P1-P6. In the preferred embodiment, a thin layer of nickel is initially deposited, followed by an overlying thin layer of gold. The deposition of such thin layers is standard in the art and can be implemented for example by dropping molten metal on to a substrate rotating at a high speed. However, other standard thin film deposition 10 techniques could be utilized. The thickness of the thin conductive film should lie in the range of about 0.5 micrometre to about 3.0 micrometres and is preferably about 1.0 micrometre.

Next, the deposited thin conductive films are 20 etched by conventional wet or dry etching techniques to form the desired conductive patterns, including the meandering conductive path segments P1A-P6A, P1B-P6B. Preferably, the width of the conductive path segments is about 25 micrometres and 25 the spacing between adjacent conductive path segments of the wire meshes WMA and WMB is also about 25 micrometres, although conductive path width and spacing as small as about 10 micrometres would be possible. The plates are now trimmed to 30 the correct size. The ceramic interconnect studs K1-K16 and L1-L16, the ceramic support studs S1-S8, T1-T8 and the interconnect blocks N1-N8, A1-A8 are produced. Conductive areas such as 34, 38 (Figure 8) on the interconnect studs K1-K8, L1-L8 and conductive 35 coatings on a pair of adjacent sides on each of the interconnect blocks N1-N8, Q1-Q8 are then formed by standard thick film deposition techniques. The ceramic interconnect studs K1-K16, L1-L16 and the support studs S1-S8, T1-T8 are then bonded to the 40 plates P1-P6 at the desired locations by using non-conductive epoxy. Next, the interconnect studs K1-K16, L1-L16 are connected to the relevant interconnection points on the plates P1-P6 by bonding into place conductive wires, such as the wires 44, 44 shown in Figure 8. The ceramic plate 82 (Figure 7) 45 having the electronic circuitry 84 mounted thereon is then mounted on the base plate P6 by means of the ceramic support studs 80. The side plates P2-P5 are then attached to the top plate P1, using non- 50 conductive epoxy, with the interconnect blocks N1-N8, Q1-Q8 being attached in their desired locations on the top and side plates P1-P5. The assembly consisting of the plates P1-P5 is then bonded to the base plate P6 to form the complete device 10.

55 It will be appreciated that since the conductive path segments of the wire meshes WMA and WMB are coplanar on each of the respective plates P1-P6, they can be readily simultaneously formed by the simple thin film deposition and etching steps referred to 60 above.

Referring now to Figure 10, the electronic circuitry 84 of Figure 7 will now be discussed in more detail. The electronic circuitry 84 includes data processing circuitry 100 and tamper detection circuitry 102.

65 The data processing circuitry 100 can be utilized to

perform any desired data processing operation in such applications as, for example, electronic payment systems, electronic fund transfers, data encryption/decryption, PIN (personal identification

- 70 number) verification, data transmission/reception, access control and home banking. The data processing circuitry 100 includes a processor 102 for selectively controlling the operation of the electronic circuitry 84 in response to input data and instructions, a timing and control circuit 104 for controlling the operation of the processor 102, a programmable read only memory (PROM) 106 for storing the software program to be executed by the processor 102, a random access memory (RAM) 108 for providing a temporary memory storage, a volatile memory 110 for permanently storing the most sensitive or secure data such as a key storage key (KSK) (to be explained), a random number generator 112 and an input/output (I/O) unit 114.
- 75 80 85 90 95 100 105 110 115 120 125 130 A data, control and address bus 116, bidirectional I/O bus 118 and I/O lines 120 and 122 are coupled to the processor 102, timing and control circuit 104, PROM 106, RAM 108 and I/O unit 114 to enable the data processing circuitry 100 to perform its data processing operations. Data may be passed over bidirectional I/O bus 118 to or from the processor 102 and over I/O lines 120 and 122 to or from the I/O unit 114. The remote ends of the I/O bus 118 and I/O lines 120 and 122 may be selectively coupled to, for example, another data processor (not shown), a main computer (not shown) and a peripheral (such as a keyboard) (not shown) via the terminals 14 (Figure 1) in order to enable the data processing circuitry 100 to perform its preselected operations.
- 100 Power to operate the electronic circuitry 84 is preferably supplied from external power sources (not shown), such as power supplies and batteries, connected to preselected ones of the terminal areas 14 (Figure 1).
- 105 An initialization subroutine, contained in the software program stored in the PROM 106, is executed in a special mode of operation controlled by an authorized person. Preferably, this initialization subroutine can only be executed once after the security device 10 (Figure 1) has been completely assembled.
- 110 For purposes of additional security it is preferable that the volatile memory 110 be, for example, a resettable memory such as a 64-bit shift register memory.
- 115 During the execution of an INITIALIZE sub-routine the processor 102 applies an INITIALIZE signal to the random number generator 112 to enable the generator 112 to generate a random number which is stored in the memory 110 as an exemplary sequence of 64 random bits. This sequence of 64 random bits is the KSK (key storage key), which is the most sensitive or secure data contained in the data processing circuitry 100. The KSK is utilized to encrypt keys which are to be entered into the security device 10 for storage in the RAM 108. Such keys are then used in data encryption operations. The precise manner in which the KSK is utilized is not of significance to the present invention and will, therefore, not be further described herein. It should, however, be noted that the resettable memory 110 stores the KSK, that the con-

tents of the memory 110 cannot be altered (if the security device 10 was programmed to run the initialization program only once), that the KSK is never outputted to the outside world from the security device 5 10, and that for purposes of security external access to the KSK contents of the memory 110 by various means must be prevented.

Tamper detection circuitry 102 is included in the electronic circuitry 84 to specifically actively destroy 10 the KSK in the resettable memory 110 if there is any attempt to penetrate the housing 11 of the security device 10 to gain access to the KSK stored in the memory 79. It should be realized that if the KSK is destroyed, any encrypted data or keys stored in RAM 15 108 become meaningless or useless. Two principal ways that someone could employ to attempt to gain access to the KSK stored in the resettable table memory 110, as well as the reaction of the tamper detection circuitry 102 to such attempts, are discussed below.

Firstly, an attempt to penetrate the ceramic housing 11 of the security device 10 may be made by drilling into or cracking the housing 11. To protect against this possibility, wire mesh A (WMA) of Figure 25 9 is connected between a supply voltage V_C and a sense circuit 124, while wire mesh B (WMB) of Figure 9 is connected between a reference potential such as ground and a sense circuit 126. It will be recalled that WMA and WMB are different conductive paths 30 formed on the interior surfaces of the plates P1-P6 forming the housing 11. An attempt to drill into or crack the housing 11 that damages either or both of WMA and WMB will be readily sensed. If WMA is broken or shorted to either WMB or ground by such 35 an attempt, sense circuit 124 will generate a low voltage signal at point 128. Similarly, if WMB is broken or shorted to either WMA or V_C by such an attempt, the sense circuit will generate a low voltage signal at point 128. In response to a low voltage signal at point 40 128, a low voltage detector 130 generates a RESET signal on a line 131 to reset the memory 110 thereby actively clearing or destroying the KSK in the resettable memory 110.

Because of the narrow width and spacing of the 45 conductive path segments on the plates P1-P6, the possibility is precluded of forming a very small diameter hole without breaking the continuity of at least one of the wire meshes WMA and WMB. The formation of such a small diameter hole could provide the 50 possibility of a security breach, for example by permitting a very thin wire to be inserted into the device 10 to make electrical contact with the electronic circuitry 84.

It is known that it is possible to retain data in static 55 CMOS cells of a memory in an unpowered state (no supply voltage or battery voltage present), if those cells are initially frozen below -90 degrees centigrade before power is removed from the memory 110. If this were done, it could be possible to subsequently forcibly break into the security device 10 and 60 read out the "frozen" contents of the memory 110.

A low temperature sensor 132 is therefore provided in the tamper detection circuitry 102 to protect the security device 10 (Figure 1) against the above-described tampering at extremely low temperatures. 65

The sensor 132 is also connected to point 128. Sensor 132 is so implemented that when the temperature within the housing 11 (Figure 1) falls to, for example, -25 degrees centigrade, the sensor 132 generates

70 and applies a low voltage signal to point 128. This low voltage signal applied from sensor 132 to point 128 will also cause the low voltage detector 130 to generate a RESET signal on the line 131 to reset the memory 110 to actively clear or destroy the KSK in 75 the memory 110.

Referring now to Figure 11, the tamper detection circuitry 102 will be described in more detail.

The tamper detection circuitry 102 essentially includes four parts. A first part includes wire mesh 80 WMA and sense circuit 124. A second part includes wire mesh WMB and sense circuit 126. A third part includes the low temperature sensor 132. All of the first, second and third parts are connected to a common output at point 128 which, in turn, is connected to the fourth part which includes the low voltage detector 130. Consequently, if any of the first, second or third parts detects any attempt to gain access to the KSK in memory 110 (Figure 10) a low output is developed at point 128. As mentioned before, such a low output at point 128 will cause the low voltage detector 130 to actively reset the memory 110 to destroy the KSK stored therein.

In the first part, pin C of WMA is coupled to sense circuit 124. A high or positive supply voltage V_C is 95 applied to pin A of WMA and to each of cascaded inverters 134 and 136 in sense circuit 124. For purposes of this discussion assume that $V_C = +4.5$ volts. A one megohm resistor 138 is connected between pin C of WMA and a low reference potential such as ground.

100 Pin C is also connected to the input of inverter 134. The output of inverter 136 is applied through a 120 kilohm resistor 140 to point 128.

When WMA is undamaged (not broken or shorted to either ground or WMB), the input to inverter 134 is 105 high, the output of inverter 134 is low and the output of inverter 136 is high.

In the second part, pin D of WMB is coupled to sense circuit 126 and pin B of WMB is connected to the low reference potential or ground. A one 110 megohm resistor 142 is connected between pin D of WMB and V_C . The supply voltage V_C is also applied to cascaded inverters 144, 146, and 148. Pin D is also connected to the input of inverter 144 which, in turn, has its output connected to the input of inverter 146.

115 The output of inverter 146 is then connected to the input of inverter 148. The output of inverter 148 is applied through a 120 kilohm resistor 150 to point 128. A 30 kilohm resistor 152 is connected between point 128 and ground to develop a common output 120 for the sense circuits 124 and 126, as well as to the low temperature sensor 132 (to be explained).

When WMB is undamaged (not broken or shorted to either V_C or WMA), the input to inverter 144 is low, the output of inverter 146 is low and the output of 125 inverter 148 is high.

Part 3 includes the low temperature sensor 132 (Figure 10). The low temperature sensor 132 includes: a negative temperature coefficient (NTC) bridge circuit 154 which includes serially-connected resistors 156 and 158 coupled between V_C and ground, 130

and serially-connected resistors 160 and 162 respectively coupled between V_C and ground; an operational amplifier 164 having its non-inverting input (+) connected to the junction of resistors 160 and 162 5 and its inverting input (-) connected to the junction of resistors 160 and 162; an inverter 166 for inverting the output of the operational amplifier 164; and a diode 168 coupled between the output of inverter 166 and the point 128.

10 The resistors 160 and 162 may be 800 kilohm resistors, while the resistors 158 and 160 may be 68 kilohm resistors having negative temperature coefficients (NTC). With this implementation the bridge circuit 154 would be unbalanced until the temperature 15 inside the housing 11 reaches approximately -25 degrees C. It can be readily seen that when the bridge circuit 154 is unbalanced, the operational amplifier 164 develops a low output which is inverted by inverter 166 to backbias the diode 168. Therefore, when 20 the temperature inside the housing 11 (Figure 1) is above -25 degrees centigrade, the low temperature sensor 132 is effectively disconnected by the back-biased diode 168 from the point 128.

Part 4 includes a low voltage detector 130 connected to point 128 for developing a RESET signal on the line 131 when the potential across resistor 152 is below a preselected threshold voltage of, for example, +1.15 volts when $V_C = +4.5$ volts, a capacitor 170 connected between point 128 and ground for retaining the input potential (voltage developed across resistor 152) to the detector 130 for a sufficient time to enable the detector 130 to generate a RESET signal when the potential across resistor 152 falls below +1.15 volts. The low voltage detector 130 may be a 35 voltage comparator which develops a low output when the voltage across resistor 152 falls below an internal reference potential of +1.15 volts.

Various conditions will now be discussed:-

(1) When no attempt has been made to freeze and/or penetrate the housing 11 to gain access to the KSK in the resettable memory 110 (Figure 10) the temperature in the housing 11 (Figure 1) will be high enough not to trigger the low temperature sensor 132 and both WMA and WMB will be undamaged. As a 45 result, the outputs of inverters 136 and 148 will both be high. Therefore, the voltage developed across resistor 152 (approximately +1.5 volts) will be above the 1.15 volt threshold of the low voltage detector 130. Consequently, the low voltage detector 130 will 50 not develop the RESET signal.

(2) When WMA is broken or shorted either to ground or WMB, pin C goes to a low potential, causing the input to inverter 134 to go low. This low input is inverted to a high signal by inverter 134. The high 55 signal (+4.5 volts) from inverter 134 is inverted by inverter 136 to a low signal (0 volts). Assume that WMB is not broken at this time and therefore that inverter 148 develops a high output (+4.5 volts). As a result, a voltage divider including resistors 140, 150 60 and 152 will cause point 128 to fall to approximately +0.9 volts. Since +0.9 volts is below the +1.15 volt threshold of the low voltage detector 130, the low voltage detector 130 will develop the RESET signal to actively reset memory 110 (Figure 10).

65 (3) When WMB is broken or shorted either to V_C or

WMA, pin D goes high (+4.5 V). This high signal is inverted by inverter 144. The low signal (0 volts) from inverter 144 is inverted by inverter 146. The high signal from inverter 146 is inverted by inverter 148.

70 Assume that WMA is not broken at this time and therefore that inverter 136 develops a high output (+4.5 volts). As a result, the voltage divider comprised of resistors 140, 150 and 152 will cause point 128 to fall to approximately +0.9 volts. This will then 75 cause the low voltage detector 130 to develop the RESET signal to reset memory 110 (Figure 10).

If both WMA and WMB are broken, the inverters 136 and 148 will both go low, causing the charge across capacitor 170 to fall toward 0 volts. However, as 80 soon as the voltage across capacitor 170 falls below +1.15 volts, the low voltage detector 130 will generate the RESET signal on the line 131.

(4) If V_C falls below +3.5 volts, the voltage across capacitor 170 will fall below +1.15 volts. This again 85 will cause the low voltage detector 130 to generate the RESET signal on the line 131.

(5) When the temperature in the housing falls below -25 degrees centigrade, the bridge circuit 154 in the low temperature sensor 132 becomes either

90 balanced or unbalanced in the opposite direction. In either event, the operational amplifier 164 develops a high output which is inverted by inverter 166. The low output (0 volts) from inverter 166 forward biases diode 168 causing point 128 to fall toward 0 volts.

95 This will cause the charge across capacitor 170 to fall toward 0 volts. However, as soon as the voltage across capacitor 170 falls below +1.15 volts, the low voltage detector 130 generates the RESET signal on the line 131 to clear the memory 110.

100 The invention thus provides a security device 10 for the secure storage of sensitive data. It provides protection for the device 10 against chemical attack, physical attack, and tampering at extremely low temperature. The ceramic housing cannot be penetrated

105 by chemicals, since ceramic material will not dissolve. Physical attack by cutting or drilling will result in the ceramic housing 11 cracking or breaking, thus breaking or damaging at least one of the two conductive paths WMA and WMB. Penetration of the 110 housing 11 by forming a very small diameter hole will result in the interruption of at least one of the wire meshes WMA and WMB. Furthermore, attempts to utilize a conductive fluid to bypass interruptions of the wire meshes will result in a short circuit between

115 the wire meshes WMA and WMB. The tamper detection circuitry 102 then actively resets the resettable memory 110 to destroy the sensitive data stored therein. Similarly, any attempt to tamper with the security device 10 at an extremely low temperature 120 will also cause the tamper detection circuitry 102 to actively reset the memory 110.

Modifications of the invention are possible. For example, if in a particular application it were envisaged that the use of a conductive fluid to bypass interruptions in the conductive path were not a practicable possibility, then the two wire meshes WMA and WMB could be replaced by a single wire mesh forming a winding configuration over the entire interior surface of the housing 11, by interconnecting winding conductive path segments on the parts P1-P6 in

the manner described hereinabove.

It will be appreciated that by forming the wire meshes WMA and WMB using thin film technology, the thin film conductive path segments forming the 5 wire meshes WMA and WMB can have a very narrow width and spacing, thereby enhancing the security of the security device. However, if a somewhat lower degree of security were deemed to be acceptable in a particular application, a modification would be possible 10 wherein the conductive path segments constituting the wire meshes WMA and WMB could be formed by thick film technology, discussed hereinabove, instead of thin film technology. Using thick film technology, a preferred width and spacing for 15 the conductive paths and spacing is about 300 micrometres, with a film thickness of about 10 micrometres.

CLAIMS

20

1. A security device for protecting stored sensitive data, including a closed housing containing memory means adapted to store sensitive data, and conductive path means provided in a winding configuration on the entire inner surface of said housing, wherein said housing contains tamper detection circuitry which is coupled to said conductive path means and to said memory means, and which includes reset signal generating means adapted to generate 25 a reset signal to erase the contents of said memory means in the event of an interruption of said conductive path means brought about by an attempt to penetrate said housing.

2. A security device according to claim 1, wherein 35 said conductive path means is formed by a conductive thin film.

3. A security device according to claim 1 or 2, wherein said conductive path means includes first and second substantially parallel conductive paths 40 provided on said inner surface of said housing.

4. A security device according to claim 3, wherein 45 said housing includes a plurality of individual parts connected together, each part including a ceramic substrate having first and second conductive path segments provided thereon, said device including interconnection means interconnecting the respective first and second conductive path segments on said plurality of individual parts to form said first and second conductive paths.

50 5. A security device according to claim 4, wherein said conductive path segments are formed by a thin conductive film having a thickness in the range of from about 0.5 micrometres to about 3.0 micrometres.

55 6. A security device according to claim 5, wherein the width of said conductive path segments is in the range of from about 10 micrometres to about 25 micrometres and the spacing between adjacent conductive path segments is in the range of from about 10 60 micrometres to about 25 micrometres.

7. A security device according to claim 6, wherein 65 interconnection means includes a plurality of individual interconnection devices, each including: first and second nonconductive members having respective first and second conductive areas provided

thereon, said first and second nonconductive members being mounted on first and second ones of said parts; conductive means interconnecting said first and second conductive areas with respective conductive path segments on said first and second parts; and a conductive member interconnecting said first and second conductive areas.

8. A security device according to claim 7, wherein 70 said conductive member includes a multi-sided block of nonconductive material provided with conductive material on two adjacent sides thereof.

9. A security device according to claim 3, wherein 75 said tamper detection circuitry includes first and second sensing means connected respectively to

80 said first and second conductive paths and responsive to damage to the respective first and second conductive paths to provide respective first and second control signals, said reset signal generating means being connected to said first and second sensing means and being adapted in response to either 85 of said first and second control signals to generate said reset signal.

10. A security device according to claim 9, wherein 90 said first conductive path has a first terminal thereof connected to power supply means and to said first sensing means and a second terminal thereof connected through a first resistor to a reference potential and wherein said second conductive path has a first terminal thereof connected through a

95 second resistor to said power supply means and to said second sensing means, and a second terminal thereof connected to said reference potential.

11. A security device according to claim 9 or 10, wherein 100 said tamper detection circuitry includes

temperature sensing means connected to said reset signal generating means and adapted, in response to a decrease in temperature within said housing below a predetermined temperature level to provide a third control signal to cause said reset signal generating

105 means to generate said reset signal.

12. A security device according to any one of the preceding claims, wherein said memory means includes a resettable shift register adapted to be reset by said reset signal.

110 13. A security device for protecting stored sensitive data, substantially as hereinbefore described with reference to the accompanying drawings.